

CLAIMS

1. A method of establishing a communication path from a first legal entity in a data communication network, comprising the steps of:
 - 5 providing at least one private reference point comprised in said data communication network,
 - establishing a communication path from said first legal entity to said private reference point,
 - verifying the authentication of said first legal entity relative to said private reference point from said first legal entity and
 - 10 establishing communication from said private reference point to a second legal entity through said data communication network without disclosing the identity of said first legal entity.
- 15 2. The method according to claim 1, further comprising a preliminary step of authenticating said first legal entity by registering biometrics, a signature, a code or any combinations thereof and/or comparing with correspondingly stored data.
- 20 3. The method according to claim 1 or 2, said first legal entity being an identity device.
4. The method according to claim 1 or 2, wherein said first legal entity is constituted by an identity card or a chip card including encrypted data, said method further comprising:
 - 25 said first legal entity receiving an encrypted key from said private reference point,
 - decrypting said encrypted key using a second stored key,
 - decrypting said encrypted data using said key.
- 30 5. The method according to any of the claims 1-4, said communication network being a personal area network, local area network, a wide area network, a global area network, the Internet, a radio network, a PSTN, a GSM network, a CDMA network, a UMTS network or any combinations thereof.

6. The method according to any of the claims 1-5, said private reference point being addressable by the authenticated holder of said first legal entity from a computer communicating with said data communication network.

5

7. The method according to any of the claims 1-6, further comprising said first legal entity allowing or blocking access to said private reference point by a third legal entity, constituting a third party.

10

8. The method according to claim 7, wherein said third legal entity is constituted by said first legal entity.

9. The method according to any of the claims 1-8, wherein said communication involves creating and negotiating an accountability path for this otherwise anonymous transaction dynamically adapted to the context risk profile.

15

10. The method according to claim 9, wherein said second legal entity establishes a procedure to identify said first legal entity or the holder of said first legal entity.

20

11. The method according to any of the claims 1-10, wherein said specific identification information is biometrics and/or name and/or digital signature and/or legal

25

12. The method according to any of the claims 1-11, further comprising: providing an identity provider and a service provider,

establishing communication from said second legal entity to said service provider,

establishing communication from said service provider to said identity

30

provider,

providing a fifth legal entity, constituted by a financial institution,

establishing communication from said service provider to said fourth legal entity,

transmitting information from said second legal entity to said service provider,
transmitting said information from said service provider to said identity
provider,

transmitting said information from said identity provider to said fifth legal
entity,

said fourth legal entity responding to said information by transmitting an
payment accept to said identity provider,

said identity provider transmitting payment accept to said service provider,
and

said service provider transmitting payment accept to said second legal entity.

13. A system for establishing a communication path from a first legal entity in a
data communication network, comprising:

at least one private reference point comprised in said data communication
network,

a communication path defined from said first legal entity to said private
reference point,

the authentication of said first legal entity being verified relative to said private
reference point from said first legal entity and

20 a path of communication established from said private reference point to a
second legal entity through said data communication network without disclosing the
identity of said first legal entity to said second legal entity.

14. The system according to claim 13, wherein said private reference point is
25 stored on a server communicating with said data communication network.

15. The system according to claim 13 or 14, wherein said communication network
is constituted by a personal area network, a local area network, a wide area
network, a radio network, a global area network, the Internet, a PSTN, a GSM
30 network, a CDMA network, a UMTS network or any combinations thereof.

16. The system according to any of the claims 13-15, wherein said first legal
entity being an identity device.

17. The system according to any of the claims 13-16, wherein said first legal entity being an identity card or a chip card including encrypted data such as a digital signature for verifying the authenticity relative to said private reference point.

5

18. The system according to any of the claims 13-17, wherein said authenticity of said first legal entity is obtained by use of biometrics and/or codes and/or digital signatures.

10

19. The system according to any of the claims 13-18, further comprising any of the features of any of the claims 1 to 12.